

Инструментарий хакера: RU32.EFI

26 Фев 2016

Илья Манусов



Проектирование технических устройств и систем нередко связано с необходимостью учета различных взаимно-противоречивых требований. Софт-индустрия — не исключение из этой закономерности: перед разработчиками приложений стоит задача своевременной поддержки новых аппаратных платформ и операционных систем и в то же время — сохранения совместимости с устаревающей, а иногда и безнадежно устаревшей инфраструктурой.

На примере [информационно-диагностической утилиты RU32](#) рассмотрим один из подходов к решению такой задачи. Эта утилита существует в версиях для 16-битной среды *MS-DOS*, а также 32/64-битных реализаций *UEFI Firmware*. На сайте разработчика, к слову сказать — сотрудника American Megatrends, аккуратно анонсированы работы над ARM-версией этой утилиты. Небольшое исследование позволит оценить существующую «кроссплатформенность от АМ!» в действии. Опыты выполнялись на виртуальных машинах в среде Oracle Virtual Box.

MS-DOS

В этом «ностальгическом» режиме, проблем совместимости обнаружено не было. Отметим, корректную динамическую ревизуализацию объектов, состояние которых изменяется во время просмотра. Речь о ячейке памяти в области переменных Legacy BIOS, по адресу 0000:046Ch, инкрементируемую по прерыванию от таймера с частотой около 18.2 Hz. В ответ на попытку просмотра переменных UEFI в среде Legacy BIOS, утилита визуализировала дамп памяти с адреса 0, не заявив о некорректности такого действия.

| Left | | | | Right | | | |
|------|---------|---------|--------|----------|---------|----------|----------------|
| Name | Size | Date | Time | Name | Size | Date | Time |
| .. | UP--DIR | 2-19-16 | 9:43a | RU32 | SUB-DIR | 2-10-16 | 9:25a |
| ru | exe | 1-01-16 | 10:22p | UC | SUB-DIR | 10-25-14 | 8:55p |
| | | | | io | sys | 40774 | 8-19-94 12:00p |
| | | | | msdos | sys | 38138 | 8-19-94 12:00p |
| | | | | autoexec | bat | 5 | 10-25-14 8:57p |
| | | | | command | com | 54869 | 8-19-94 12:00p |
| | | | | config | sys | 2 | 10-25-14 8:56p |
| | | | | ru | set | 1626 | 2-19-16 9:59a |

.. UP--DIR 2-19-16 9:43a RU32 SUB-DIR 2-10-16 9:25a

C:\RU32\DOS>
1Help 2Menu 3View 4Edit 5Copy 6RenMov 7Mkdir 8Delete 9PullDn 10Quit

Рис.1. На виртуальной машине загружена операционная система MS-DOS и Volkov Commander

```

File Config Go Tools System Quit                                blogspot.tw >>> Download lat
Disk / partition list                                           Page #01
Disk INT13 Drive 80h ATA                                       524MB MBR
Type:UEFI Variables Name:
Home/End/CtrlHome/CtrlEnd/PgDn/PgUp - Move, CtrlF - Find, ENTER - Done 09:48:53

```

Рис.2. Список устройств хранения данных (mass storage)

```

File Config Go Tools System Quit                                ot.tw >>> Download latest RU
Address: 0000000000000400
00 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Refresh : ON
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 C0 9F .
10 00000000 7F 02 00 00 00 00 00 00 2C 00 2C 00 0D 1C .P.P.H...P...
20 E0 50 E0 50 E0 48 0D 1C E0 50 0D 1C 0D 1C 00 00 .
30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .
40 00 80 00 00 00 00 00 00 00 00 00 03 50 00 00 10 00 00 .P...
50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .
60 00 20 00 D4 03 00 00 00 05 81 8E 00 7C FB 09 00 .
70 00 00 00 00 00 01 C0 00 00 00 00 00 00 00 00 00 00 .
80 1E 00 3E 00 18 10 00 60 F9 51 08 00 00 00 00 00 00 .>...Q...
90 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 .
A0 00 00 00 00 00 00 00 00 00 D1 53 00 C0 00 00 00 00 .S...
B0 00 00 00 00 00 00 00 00 00 01 42 01 00 00 00 00 00 .B...
C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .
D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .
E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .
F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .
Type:Memory Address 0000000000000400
<PgDn>/<PgUp> +/- 100h bytes 09:58:10

```

Рис.3. Просмотр блока переменных Legacy BIOS

```

File Config Go Tools System Quit                                ruexe.blogspot.tw
Name Vendor Device Bus# Dev# Fun#
D0:F0 Intel 82441FX MARS Pentium Pro to PCI 8086 1237 00 00 00
D1:F0 Intel 82371SB PCI-ISA ISA bridge 8086 7000 00 01 00
D1:F1 Intel PIIX4 IDE controller 8086 7111 00 01 01
D2:F0 UGA controller 80EE BEEF 00 02 00
D3:F0 AMD 79C970 Ethernet controller 1022 2000 00 03 00
D4:F0 System Peripherals 80EE CAFE 00 04 00
D7:F0 Intel 82371AB Power Management Bridge 8086 7113 00 07 00
Type:SMBIOS Handle 0000
Home/End/CtrlHome/CtrlEnd/PgDn/PgUp - Move, CtrlF - Find, ENTER - Done 09:53:30

```

Рис.4. Список PCI устройств

```

File Config Go Tools System Quit m ruexe.blogspot.tw >>> Down

00 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Refresh : ON
0000 04 00 DD 54 F4 06 70 00 CF 02 5B 13 F4 06 70 00 .T.p...X.p.
0010 00000100 00 53 FF 00 F0 DC E9 00 F0 53 FF 00 F0 .p.S.....S...
0020 3C 00 BB 0D 96 56 8D 18 53 FF 00 F0 6F 00 BB 0D <...U.S...o...
0030 87 00 BB 0D C4 01 25 34 B7 00 BB 0D F4 06 70 00 .....%4.....p.
0040 22 00 00 C0 4D F8 00 F0 41 F8 00 F0 74 07 70 00 "...M...A...t.p.
0050 39 E7 00 F0 4A 08 70 00 2E E8 00 F0 D4 EF 00 F0 9...J.p.....
0060 A4 F0 00 F0 FB 07 70 00 6E FE 00 F0 7E 56 8D 1B .....p.n...~U.
0070 ED EF 00 F0 53 FF 00 F0 22 05 00 00 ED 57 00 C0 .....S.....W..
0080 CC 40 19 00 8B 04 72 0F B1 02 8C 12 7E 56 8D 1B .e....r.....~U.
0090 7E 56 8D 18 E5 42 19 00 6C 43 19 00 DB 04 72 0F ~U...B...lC....r.
00A0 D2 40 19 00 62 07 70 00 D2 40 19 00 D2 40 19 00 .e..b.p..e...e..
00B0 D2 40 19 00 D2 40 19 00 3F 01 30 0E 9F 01 31 0E .e...e..?.0...1.
00C0 EA D3 40 19 00 FF 00 F0 D2 40 19 00 D2 40 19 00 ..e.....e...e..
00D0 06 03 EC 34 06 03 EC 34 06 03 EC 34 06 03 EC 34 ...4...4...4...4
00E0 06 03 EC 34 06 03 EC 34 06 03 EC 34 06 03 EC 34 ...4...4...4...4
00F0 06 03 EC 34 06 03 EC 34 C6 03 EC 34 D2 40 19 00 ...4...4...4.e..

Type:UEFI Variables Name:
<TAB>/<SHIFT-TAB> Next/Prev group of registers 09:54:48

```

Рис.5. Режим UEFI variables. В Legacy контексте, визуализируется область памяти с адреса 0

```

File Config Go Tools System Quit ruexe.blogspot.tw

SMBIOS Handle:00/09 Type:00 Size:38 Addr:E1000

00-BIOS Information
00 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Refresh : ON
00 00 14 00 00 01 02 00 E0 03 01 90 80 01 48 00 00 .H...
10 00000000 00 69 6E 6E 6F 74 65 6B 20 47 6D 62 48 ...innotek GmbH
20 00 56 69 72 74 75 61 6C 42 6F 78 00 31 32 2F 30 .VirtualBox.12/0
30 31 2F 32 30 30 36 00 00 01 1B 01 00 01 02 03 04 1/2006.....
D3 03 DB A7 37 5C 45 AA B6 5C 8F A3 55 26 E7 0E ....?NE...N...U&..
06 00 05 69 6E 6E 6F 74 65 6B 20 47 6D 62 48 00 ...innotek GmbH.
56 69 72 74 75 61 6C 42 6F 78 00 31 2E 32 00 30 VirtualBox.1.2.0
00 56 69 72 74 75 61 6C 20 4D 61 63 68 69 6E 65 .Virtual Machine
00 00 02 0F 08 00 01 02 03 04 00 01 00 03 00 0A .....
00 4F 72 61 63 6C 65 20 43 6F 72 70 6F 72 61 74 .Oracle Corporat
69 6F 6E 00 56 69 72 74 75 61 6C 42 6F 78 00 31 ion.VirtualBox.1
2E 32 00 30 00 00 03 0D 03 00 01 01 00 00 00 03 .2.0.....
03 03 03 4F 72 61 63 6C 65 20 43 6F 72 70 6F 72 ...Oracle Corpor
61 74 69 6F 6E 00 00 7E 2A 07 00 01 03 B1 02 76 ation..*.....o
06 01 00 FF FB EB 0F 03 02 00 00 B8 0B B8 0B 41 .....A
04 FF FF FF FF FF FF 00 00 00 01 01 01 04 00 00 .....

Type:SMBIOS Handle 0000
<0-9,A-F> Value, <Arrows> Move, <ESC> Cancel 09:51:28

```

Рис.6. Информация о BIOS виртуальной машины, предоставляемая функциями SMBIOS

UEFI IA32

В этом режиме, для обеспечения работоспособности утилиты в среде *Oracle Virtual Box*, потребовалась настройка виртуальной среды, причем достаточно радикальная. Утилита «зависала» с темным экраном. В целях совместимости, пришлось отказаться от аппаратной виртуализации (см. рис.7). Как и следовало ожидать, производительность в режиме программной виртуализации значительно ниже, это заметно по плавному скроллингу в *UEFI Shell*. Вместе с тем, даже в режиме программной виртуализации, скорость обновления экрана в утилите *RU32* достаточно высокая, что говорит о хорошей оптимизации кода. Отметим, что несовместимость замечена только при запуске конкретной версии *RU32.EFI (RU5.16.0248)* в сочетании с конкретной версией *Oracle Virtual Box (версии 5.0.10 r1040b1)*.

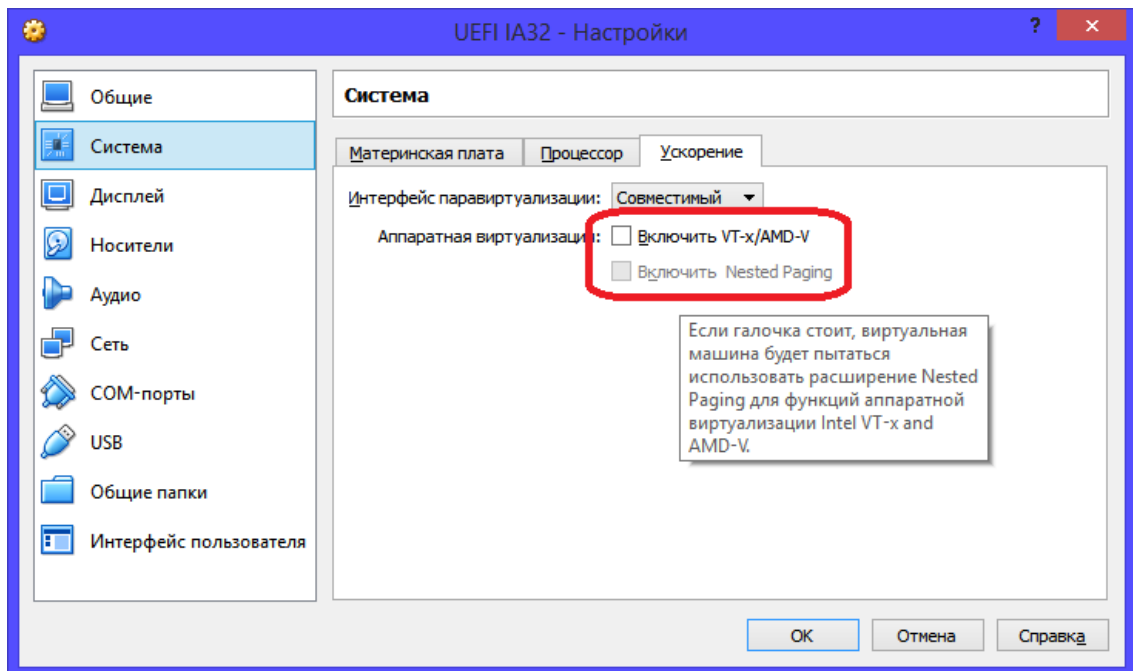


Рис.7. Отключаем аппаратную виртуализацию VT-x и опцию управления страницами Nested Paging

Настроив виртуальную машину, приступаем к исследованиям. Пытаясь увидеть переменные Legacy BIOS в режиме UEFI, получаем блок нулевых байтов (Рис.10). Отметим, что такой «разрыв с прошлым» имеет место не на всех платформах. Блок UEFI variables (рис.12) более гибок, как в смысле размещения переменных, так и с точки зрения их статуса. *NV* означает *Non Volatile* статус, *BS (Boot Services)* означает доступность переменной только на фазе загрузки ОС, до вызова системной функции *ExitBootServices()*. *RT (Runtime Services)* означает доступность переменной в сеансе ОС. Так как оболочка UEFI Shell не вызывает функцию *ExitBootServices()*, видимо не претендуя на статус полноценной операционной системы, переменные и API со статусом *BS*, доступны UEFI приложениям.

```

fs0:\> map
Device mapping table
  fs0  :HardDisk - Alias hd20b blk0
        Acpi (PNP0A03.0) /Pci (D10) /?/HD (Part1,SigEF09EF09)
  blk0 :HardDisk - Alias hd20b fs0
        Acpi (PNP0A03.0) /Pci (D10) /?/HD (Part1,SigEF09EF09)
  blk1 :HardDisk - Alias (null)
        Acpi (PNP0A03.0) /Pci (D10) /?/HD (Part2,SigEF09EF09)
  blk2 :HardDisk - Alias (null)
        Acpi (PNP0A03.0) /Pci (D10) /?/HD (Part2,SigEF09EF09) /HD (Part1,Sig00000000)
  blk3 :BlockDevice - Alias (null)
        Acpi (PNP0A03.0) /Pci (111) /Ata (Secondary,Master)
  blk4 :BlockDevice - Alias (null)
        Acpi (PNP0A03.0) /Pci (D10) /?
  hd20b :HardDisk - Alias fs0 blk0
        Acpi (PNP0A03.0) /Pci (D10) /?/HD (Part1,SigEF09EF09)

fs0:\> ver
EFI Specification Revision : 2.31
EFI Vendor                 : EDK II
EFI Revision               : 1.0
EFI Build Version         : 20061109

fs0:\>

```

Рис.8. На виртуальной машине загружен UEFI Shell для IA32 UEFI

```

File Config Go Tools System Quit                               ruexe.blogspot.tw
Disk / partition list                                         Page #01
Disk 26.845GB MBR
Partition #1 41MB
Partition #2 26.799GB

Type:PCI Bus 00 Device 00 Function 00
ome/End/CtrlHome/CtrlEnd/PgDn/PgUp - Move, CtrlF - Find, ENTER - Done 10:29:31

```

Рис.9. Список устройств хранения данных (mass storage)

```

File Config Go Tools System Quit                               ruexe.blogspot.tw >>> Downl
Address: 0000000000000400

00 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Refresh : ON
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
10 00000000 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

Type:Memory Address 0000000000000400
<Ctrl-Right><Ctrl-Left> Next/Prev config, <Space> toggle binary 10:30:43

```

Рис.10. Просмотр переменных Legacy BIOS по адресу 0000:0400h. В контексте UEFI этот блок не используется и обнулен

| Name | Vendor | Device | Bus# | Dev# | Fun# |
|---|--------|--------|------|------|------|
| 00:F0 Intel 82441FX MARS Pentium Pro to PCI | 8086 | 1237 | 00 | 00 | 00 |
| D1:F0 Intel 82371SB PCI-ISA ISA bridge | 8086 | 7000 | 00 | 01 | 00 |
| D1:F1 Intel PIIX4 IDE controller | 8086 | 7111 | 00 | 01 | 01 |
| D2:F0 VGA controller | 80EE | BEEF | 00 | 02 | 00 |
| D3:F0 AMD 79C970 Ethernet controller | 1022 | 2000 | 00 | 03 | 00 |
| D4:F0 System Peripherals | 80EE | CAFE | 00 | 04 | 00 |
| D5:F0 Intel ICH (Audio) Audio device | 8086 | 2415 | 00 | 05 | 00 |
| D6:F0 USB OHCI | 106B | 003F | 00 | 06 | 00 |
| D7:F0 Intel 82371AB Power Management Bridge | 8086 | 7113 | 00 | 07 | 00 |
| D13:F0 Intel AHCI 1.0 controller | 8086 | 2829 | 00 | 0D | 00 |

Type:PCI Bus 00 Device 00 Function 00
Home/End/CtrlHome/CtrlEnd/PgDn/PgUp - Move, CtrlF - Find, ENTER - Done 10:31:48

Рис.11. Снимок PCI устройств

| UEFI Variable Name | Attributes | GUID | Page #01 |
|---------------------------|------------|-----------------------------|----------|
| GRP | BS | 47C7B226-C42A-11D2-8E5700A0 | |
| ARPSb | BS | 47C7B226-C42A-11D2-8E5700A0 | |
| BackgroundClear | BS+RT | 4D1EDE05-38C7-4A6A-9CC64BCC | |
| blk0 | BS | 47C7B225-C42A-11D2-8E5700A0 | |
| blk1 | BS | 47C7B225-C42A-11D2-8E5700A0 | |
| blk2 | BS | 47C7B225-C42A-11D2-8E5700A0 | |
| blk3 | BS | 47C7B225-C42A-11D2-8E5700A0 | |
| blk4 | BS | 47C7B225-C42A-11D2-8E5700A0 | |
| BlkIo | BS | 47C7B226-C42A-11D2-8E5700A0 | |
| boot-args | BS+RT | 7C436110-AB2A-4BBB-AB80FE41 | |
| Boot0000 | NU+BS+RT | EFI_GLOBAL_VARIABLE_GUID | |
| Boot0001 | NU+BS+RT | EFI_GLOBAL_VARIABLE_GUID | |
| Boot0002 | NU+BS+RT | EFI_GLOBAL_VARIABLE_GUID | |
| BootCurrent | BS+RT | EFI_GLOBAL_VARIABLE_GUID | |
| BootOptionSupport | BS+RT | EFI_GLOBAL_VARIABLE_GUID | |
| BootOrder | NU+BS+RT | EFI_GLOBAL_VARIABLE_GUID | |
| BusSpecificDriverOverride | BS | 47C7B226-C42A-11D2-8E5700A0 | |
| ComponentName | BS | 47C7B226-C42A-11D2-8E5700A0 | |
| Configuration | BS | 47C7B226-C42A-11D2-8E5700A0 | |

Type:PCI Bus 00 Device 00 Function 00
<PgDn>/<PgUp>/<Home>/<End>/<Ctrl><Home>/<Ctrl><End> Move 10:32:44

Рис.12. Режим UEFI variables. Просмотр переменных UEFI Firmware

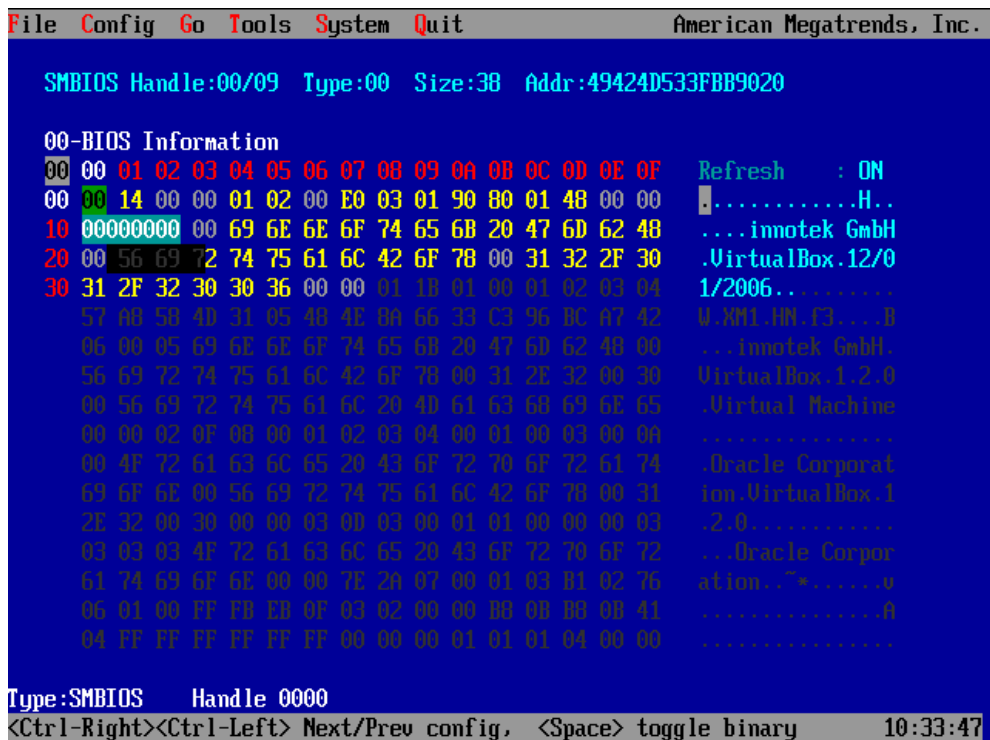


Рис.13. Информация о BIOS виртуальной машины, предоставляемая функциями SMBIOS

UEFI x64

Работоспособность утилиты RU32 в виртуальной среде UEFI x64, также зависит от установки опций Oracle Virtual Box. Но в отличие от 32-битного варианта, такие радикальные меры, как переход от аппаратной виртуализации к программной, здесь не потребовались. Ключевым моментом является тип южного моста системной логики. Если выбран относительно современный мост ICH9 включается поддержка архитектуры шины PCI Express на виртуальной платформе, при этом регистры конфигурационного пространства адресуются в адресном пространстве памяти, как *Memory Mapped I/O*. Предположительно, именно этот фактор вызывает конфликт при запуске RU32. Выбор менее современного моста PIIX3, позволяет запустить утилиту RU32 на виртуальной машине.

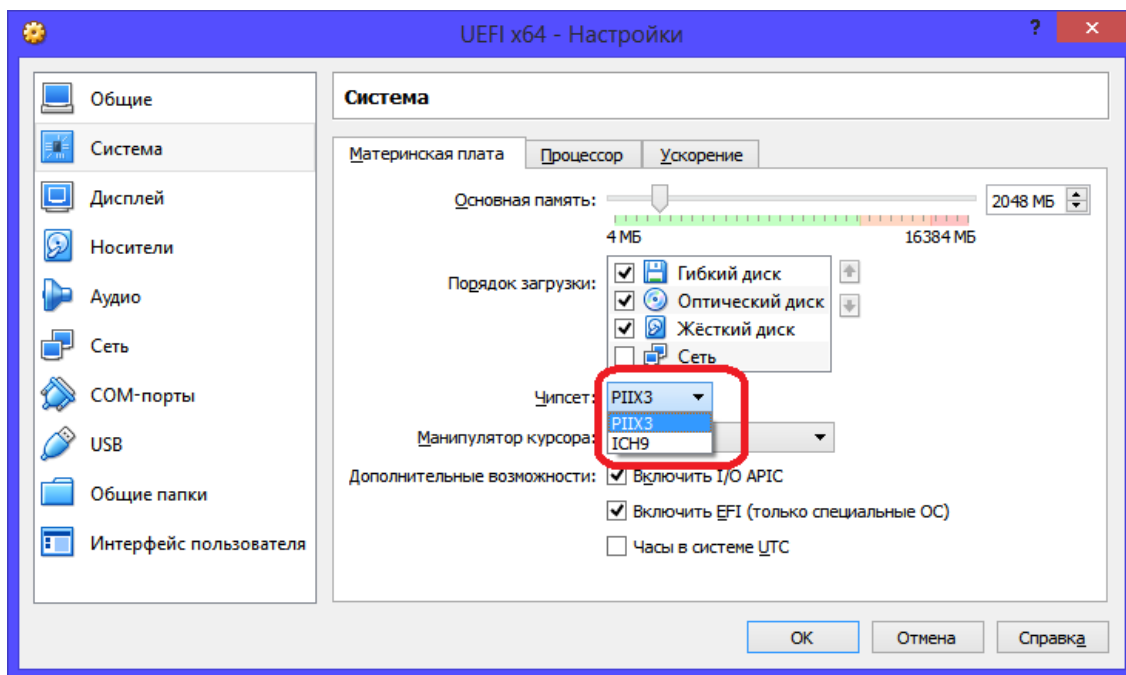


Рис.14. Выбираем модель южного моста системной логики. Полезным побочным эффектом от установки режима PIIX3, является переход к классическому методу адресации конфигурационного пространства, при этом диапазон Memory Mapped Configuration (MCFG) на виртуальной платформе отсутствует

Не будем приводить аналогичный набор скрин-шотов для UEFI x64, поскольку их содержимое практически совпадает со снимками, сделанными в режиме UEFI IA32. Вместо этого акцентируем внимание на ресурсах, состояние которых в 32 и 64-битном режиме различно. Рассмотрим дамп Model-Specific регистров процессора.

```

File Config Go Tools System Quit                                     ruexe.blogspot.tu

MSR: SMRR_PHYS_MASK

                                00 01 02 03 04 05 06 07   Refresh   : ON
TIME_STAMP_COUNT:00000010 DA 62 E2 4C 07 00 00 00   .b.L....
IA32_PLATFORM_ID:00000017 00 00 00 00 00 00 18 00   .....
IA32_APIC_BASE:0000001B 00 09 E0 FE 00 00 00 00   .....
EBL_CR_POWERON:0000002A 00 00 00 00 00 00 00 00   .....
PIC_MSG_CONTROL:0000002E 00 00 00 00 00 00 00 00   .....
DCU_MODE:00000031 00 00 00 00 00 00 00 00   .....
CORE_MTHREAD_COU:00000035 01 00 01 00 00 00 00 00   .....
SOCKET_ID:00000039 00 00 00 00 00 00 00 00   .....
IA32_FEATURE_CON:0000003A 01 00 00 00 00 00 00 00   .....
IA32_TEMPERATURE:0000003F 00 00 00 00 00 00 00 00   .....
ULW_CONTROL:0000004B 00 00 00 00 00 00 00 00   .....
IA32_BIOS_UPDT_T:00000079 00 00 00 00 00 00 00 00   .....
IA32_BIOS_SIGN_I:0000008B 00 00 00 00 00 00 00 00   .....
IA32_SMM_MONITOR:0000009B 00 00 00 00 00 00 00 00   .....
SMRR_PHYS_BASE:000000A0 00 00 00 00 00 00 00 00   .....
SMRR_PHYS_MASK:000000A1 00 00 00 00 00 00 00 00   |.....
                                00000000

Type: Intel CPU MSRs   CPU# 00
Hex to change value, <ENTER> Write MSRs, <ESC> Abort                                     12:46:03

```

Рис.15. Дамп Model-Specific регистров в режиме IA32 UEFI

```

File Config Go Tools System Quit                                     American Megatrends, Inc.

MSR: RESERVED - SMRR_PHYS_MASK

                                00 01 02 03 04 05 06 07   Refresh   : ON
TIME_STAMP_COUNT:00000010 99 EE B0 5C 10 00 00 00   ...\.
IA32_PLATFORM_ID:00000017 00 00 00 00 00 00 18 00   .....
IA32_APIC_BASE:0000001B 00 09 E0 FE 00 00 00 00   .....
EBL_CR_POWERON:0000002A 00 00 00 00 00 00 00 00   .....
PIC_MSG_CONTROL:0000002E 00 00 00 00 00 00 00 00   .....
DCU_MODE:00000031 FF FF FF FF FF FF FF FF   .....
CORE_MTHREAD_COU:00000035 01 00 01 00 00 00 00 00   .....
SOCKET_ID:00000039 FF FF FF FF FF FF FF FF   .....
IA32_FEATURE_CON:0000003A 01 00 00 00 00 00 00 00   .....
IA32_TEMPERATURE:0000003F FF FF FF FF FF FF FF FF   .....
ULW_CONTROL:0000004B FF FF FF FF FF FF FF FF   .....
IA32_BIOS_UPDT_T:00000079 FF FF FF FF FF FF FF FF   .....
IA32_BIOS_SIGN_I:0000008B 00 00 00 00 00 00 00 00   .....
IA32_SMM_MONITOR:0000009B 00 00 00 00 00 00 00 00   .....
SMRR_PHYS_BASE:000000A0 FF FF FF FF FF FF FF FF   .....
SMRR_PHYS_MASK:000000A1 FF FF FF FF FF FF FF FF   |.....
                                11111111

Type: Intel CPU MSRs   CPU# 00
<Ctrl> + <PgDn>/<PgUp> Select CPU number                                     12:44:02

```

Рис.16. Дамп Model-Specific регистров в режиме x64 UEFI

Регистр `TIME_STAMP_COUNT` является счетчиком процессорных тактов, его состояние постоянно изменяется, различные значения в 32 и 64 битном варианте связаны только с этим фактом. Здесь мы еще раз убедились в способности RU32 адекватно визуализировать объекты, состояние которых изменяется во время просмотра. Обратим внимание на несколько регистров, содержимое которых в 32-битном режиме — нулевое, а в 64-битном — максимальное (FFFFFFFFFFFFFFFFh). Например, регистр термоконтроля `IA32_TEMPERATURE`. Предположительно, RU32, в случае недоступности регистра, визуализирует это значение. Отметим, что более информативно было бы сообщить о недоступности регистра явно (не ограничиваясь неочевидным

комментарием над дампом), иначе получаем некоторую неопределенность, ведь регистр может быть доступен и при этом содержать данное значение.

Вместо послесловия: цель оправдывает средства

Эффективный инструмент низкоуровневого исследования платформ по определению не может быть бесконфликтным. Утилита предназначена для профессионального применения, специалистами, которые знают, чего они хотят и что для этого надо сделать. Блокировать некоторые возможности, находящиеся на границе устойчивости, чтобы защитить хакеров от самих себя, было бы неверно.